CLAIMS:

1. A process for validating a state of a storage area network (SAN), comprising:

defining a SAN access path policy representative of SAN logical access paths, said SAN logical access paths defining end-to-end access relationship between an application on a server and data LUNs stored on storage devices in the SAN and having logical access path attributes with attribute values,

collecting configuration information from devices of the SAN, standardizing formats of the configuration information and reconciling any conflicts,

processing the collected configuration information to identify the SAN logical access paths, and computing the associated attribute values,

comparing the identified SAN logical access paths and computed attribute values with the SAN access path policy to identify any logical path discrepancies or violations.

2. The process of claim 1, and further including identifying a logical access path violation if at least one identified SAN logical access path is in disagreement with the SAN access path policy.

3. The process of claim 1, and further including defining a SAN notification policy for notifying a user about SAN logical access path violations.

4. The process of claim 3, wherein notifying a user includes sending a message to the user with violation information, said message selected from the group consisting of email, graphic text and SNMP messages.

5. The process of claim 1, and further including identifying partial logical access paths, and comparing logical access path values of the partial path with the SAN logical access path policy.

6. The process of claim 1, wherein said configuration information includes device properties selected from the group consisting of server ID, server port configuration, switch port configuration, switch ID, switch IP and domain ID, grouping of devices, zoning of devices, storage device ID, LUNs of storage devices, and LUN masks.

7. The process of claim 1, wherein a logical access path attribute comprises an attribute selected from the group consisting of level of redundancy, type of redundancy, number of hops, number of allocated ports, bandwidth, component interoperability, proximity constraints, and type of component authentication.

8. The process of claim 1, and further comprising user-defined grouping of at least two logical access paths that share at least one of the logical path attribute value or are within a range of predefined logical path attribute values.

9. The process of claim 1, wherein collecting configuration information includes polling a SAN device API, simulating a CLI session with a SAN device, communicating with a SAN device using a CIM or SNMP protocol, or a combination thereof.

10. The process of claim 1, and further comprising validating a change state event of the SAN by

collecting SAN event description information, and

processing the SAN event description information to identify SAN logical access paths that have attribute values that do not comply with the SAN access path policy, thereby indicating a changed state of the SAN.

11. A process for validating a state change event of a storage area network (SAN), comprising:

defining a SAN access path policy representative of SAN logical access paths,

defining a SAN state based on SAN logical access paths and attribute values associated with the logical access paths,

obtaining SAN event description information, and

comparing the SAN event description information with the SAN state to identify a any logical path discrepancies or violations.

12. The process of claim 11, and further defining a SAN change plan and comparing the SAN event description information with the SAN change plan.

13. The process of claim 11, wherein the SAN change event is selected from the group consisting of an erroneous change in a SAN device configuration, a planned change in a SAN device configuration and a device failure.

14. The process of claim 11, wherein the SAN event description is obtained by at least one of polling, trapping after an event occurs, by a direct administrator input, by an input from a provisioning system about an intended change, by intercepting a change command before an event occurs.

15. A storage area network (SAN) validation manager, comprising:

a policy engine that stores a SAN access path policy representative of SAN logical access paths, said SAN logical access paths defining end-to-end access relationship between an application on a server and data LUNs stored on storage devices in the SAN and having logical access path attributes with attribute values,

a validation engine that collects configuration information from devices of the SAN, standardizes formats of the configuration information and reconciles any conflicts, The

validation engine further processing the collected configuration information to identify the SAN logical access paths and computing the associated attribute values, and comparing the identified SAN logical access paths and computed attribute values with the SAN access path policy to identify any logical path discrepancies or violations.

16. The SAN manager of claim 15, further comprising a change engine that collects SAN event description information, and processes the SAN event information to identify SAN logical access paths that have attribute values that do not comply with the SAN access path policy, thereby indicating a changed state of the SAN.